(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 December 2001 (13.12.2001)

PCT

(10) International Publication Number
WO 01/95590 A1

(51) International Patent Classification[7]: H04L 29/06, 12/26

(21) International Application Number: PCT/EP01/06247

(22) International Filing Date: 1 June 2001 (01.06.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
1015389 7 June 2000 (07.06.2000) NL

(71) Applicant *(for all designated States except US)*: KONINKLIJKE KPN N.V. [NL/NL]; Stationsplein 7, NL-9726 AE Groningen (NL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: DIJKSTRA, Willem, Pieter [NL/NL]; Fongerplaats 165, NL-9725 LK Groningen (NL). VAN STEENBERGEN, Ate, Sander [NL/NL]; Framaheerd 82, NL-9737 NN Groningen (NL).

(74) Agent: WUYTS, Koenraad, Maria; Koninklijke KPN N.V., P.O. Box 95321, NL-2509 CH The Hague (NL).

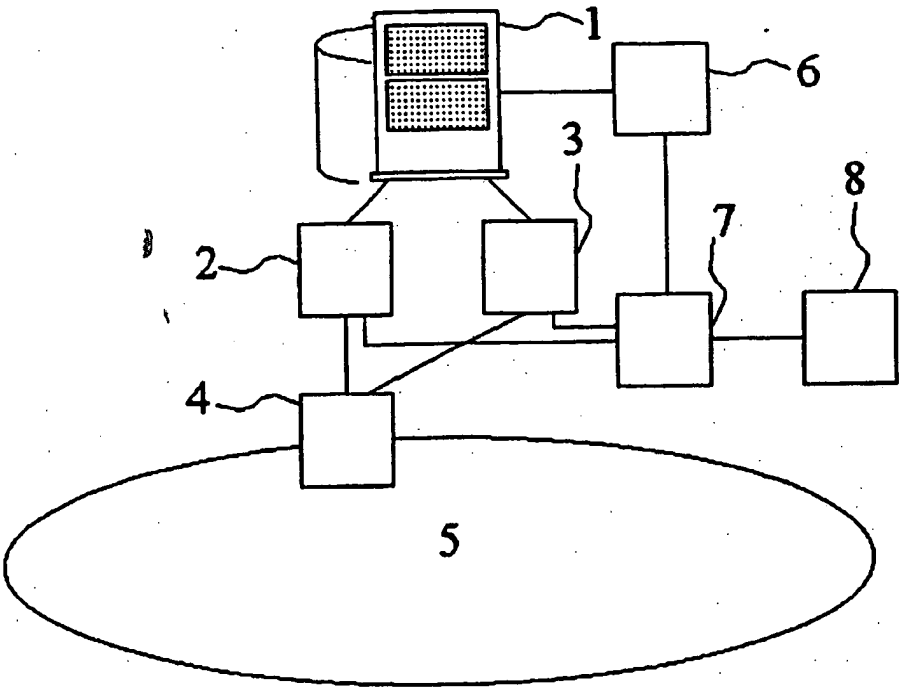
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:
— *of inventorship (Rule 4.17(iv)) for US only*
— *of inventorship (Rule 4.17(iv)) for US only*

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR SECURING A DATA SYSTEM



(57) Abstract: Method and system for securing a data system (1) that is connected to other systems by communication means (5) and exchanges data with these other systems via said communication means. The most recently exchanged data is continuously buffered in buffer devices (2, 3). The normal operation of the data system is monitored by a monitoring device (6) that in the event of an abnormality in the operation of the data system activates an output device (7) in order to read out the buffered data from the buffer devices and to make these data available for analysis.

WO 01/95590 A1

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Method and system for securing a data system

BACKGROUND OF THE INVENTION

The invention relates to a method for securing a data system that is connected by communication means to other systems and exchanges data with those other systems via said communication means. The invention also relates to a security system for monitoring a data system that exchanges data with other systems via communication means.

Present-day (Internet) security tools can only identify known attacks against a data system. Unknown attacks are not identified and can disrupt services. So-called network sniffers can log all the traffic on a network. As the bandwidths in the networks increase, however, sniffers deliver an enormous quantity of information, which makes it impossible to examine all the sniffed traffic on arrival. "Intrusion Detection Systems" are tools which, on top of a sniffer, attempt in real time to correlate network streams in the search for attacks. Drawbacks: the increased speeds and bandwidths on networks make the deployment of these tools more and more difficult. At gigabit network speeds, there are no systems still able to accomplish this task.

SUMMARY OF THE INVENTION

The present invention is based on the understanding that only at the moment that a data system malfunctions, for example as a result of a "data attack", is it important for the last communication with the server to be preserved (comparable to the "black box" in aircraft). This recorded communication can then be used to analyse and ascertain the cause of the malfunctioning and to identify a possible new attack and to secure the data system against it.

The method according to the invention is characterised in that (only) the most recently exchanged data are continuously buffered, the normal operation of the data system is monitored, and (only) in the event of an abnormality in the operation of the data system the buffered data are made available for analysis. A "moving window" is, as it were, placed over the exchanged (incoming and/or outgoing) data stream, the contents of which are not normally processed (analysed). Only after an abnormality has been detected in the operation of the data system being secured are the contents of the moving window preserved so they can be analysed. The invention therefore solves the problem of the large quantity of information and limited analysis time by not performing analysis continuously, but only when necessary.

EMBODIMENTS

The method according to the invention is illustrated with the aid of figure 1. Figure 1 shows a data system 1, provided with an input buffer device 2 and an output buffer device 3, by means of which the data system 1 connects to the node 4 of a network 5 to which other (data) systems can be connected, with which the data system 1 exchanges data. The data system is secured by buffering the most recently exchanged data in the buffer devices 2 and 3. The normal operation of the data system 1 is monitored in a monitoring device 6. The monitoring device 6 controls an output device 7 such that only in the event of an abnormality in the operation of the data system will the most recent data, buffered in the buffer devices 2 and 3, be called up by the output device 7. The output device 7 may comprise a screen on which, after a fault has occurred in the data system, the data called up from the buffers 2 and 3 can be examined. The output device 7 can also comprise a printer. A "moving window" is, as it were, placed over the exchanged (incoming and/or outgoing) data stream, the contents of which are not normally processed (analysed). Only after an abnormality has been detected in the operation of the data system being secured are the contents of the moving window (in the buffer devices 2 and 3 respectively) preserved so they can be analysed. The data exchanged in the last moments before the occurrence of the fault can be analysed visually by qualified personnel. Alternatively, an analysis system 8 can be used, possibly in addition to the aforementioned method.

It should be noted that securing the data system 1 can also be achieved remotely, for example via the network 5, as shown in figure 2. In figure 2 the required connections between the devices 1, 2 and 3 on the one hand and the devices 6 and 7 on the other are accomplished via the network node 4 and a network node 9. These connections are, of course, depending on the network, preferably accomplished by virtual channels. The devices 6, 7 and 8 can form part of a security server 10, as shown in figure 3, which can monitor a large number of data systems 1. The behaviour of the data systems 1 to be secured is monitored in real time from security server 10, which receives information from the data systems 1 to be protected. If a data system 1 displays deviant behaviour, the contents of the buffer devices 2 and 3 are "tapped" and examined by the security server, possibly with aid of automated analysis means, such as device 8 in figure 2.

It is pointed out that where the above description mentions two

buffer devices, 2 and 3, one for incoming data and one for outgoing data, these functions can in practice also be performed by a single input/output buffer. Should a disaster occur in the operation of the data system 1, this I/O buffer will then be read out and the communication data present therein at that moment will be made available to the device 7.

Deviant behaviour of a data system 1 can for example be: a characteristic quantity deviating from its statistical value, a peak load, a continuous very high load, a hard disk becoming full, active processes failing, etc.

The analysis could be used for:

* Forensic examination and solving questions of guilt, etc.
* Identification of (unknown) "network attacks"; the information thus obtained could then be used to protect the data systems even better.

CLAIMS

1. Method for securing a data system that is connected by communication means to other systems and exchanges data with those other systems via said communication means, characterized in that the most recently exchanged data are continuously buffered, the normal operation of the data system is monitored, and in the event of an abnormality in the operation of the data system the buffered data are made available for analysis.

2. Security system for monitoring a data system (1) that exchanges data with other systems via communication means (5), characterized by buffer means (2,3) for the continuous buffering of the data most recently exchanged by the data system and by output means (7) for making the buffered data available.

3. Security system according to claim 2, characterized by monitoring means (6) for monitoring the data system for normal operation and for activating the output means (7) in the event of abnormality in the operation of the data system.

4. Security system according to claim 3, characterized by analysis means (8) for analysing the data made available by the activated output means (7).

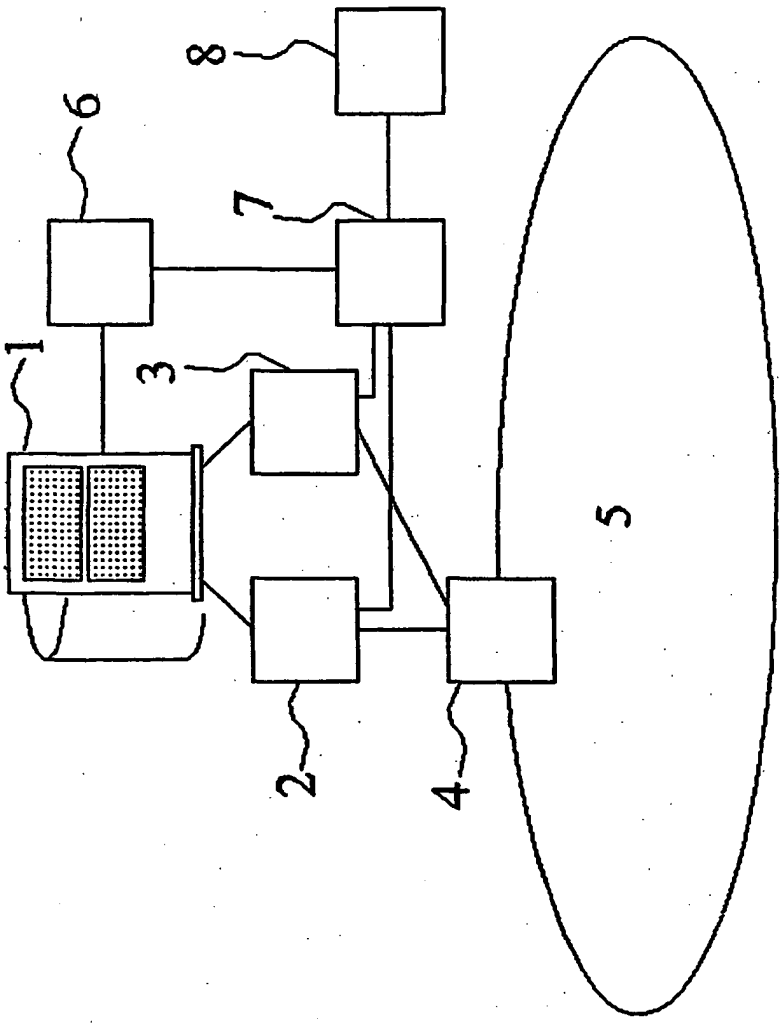


FIG. 1

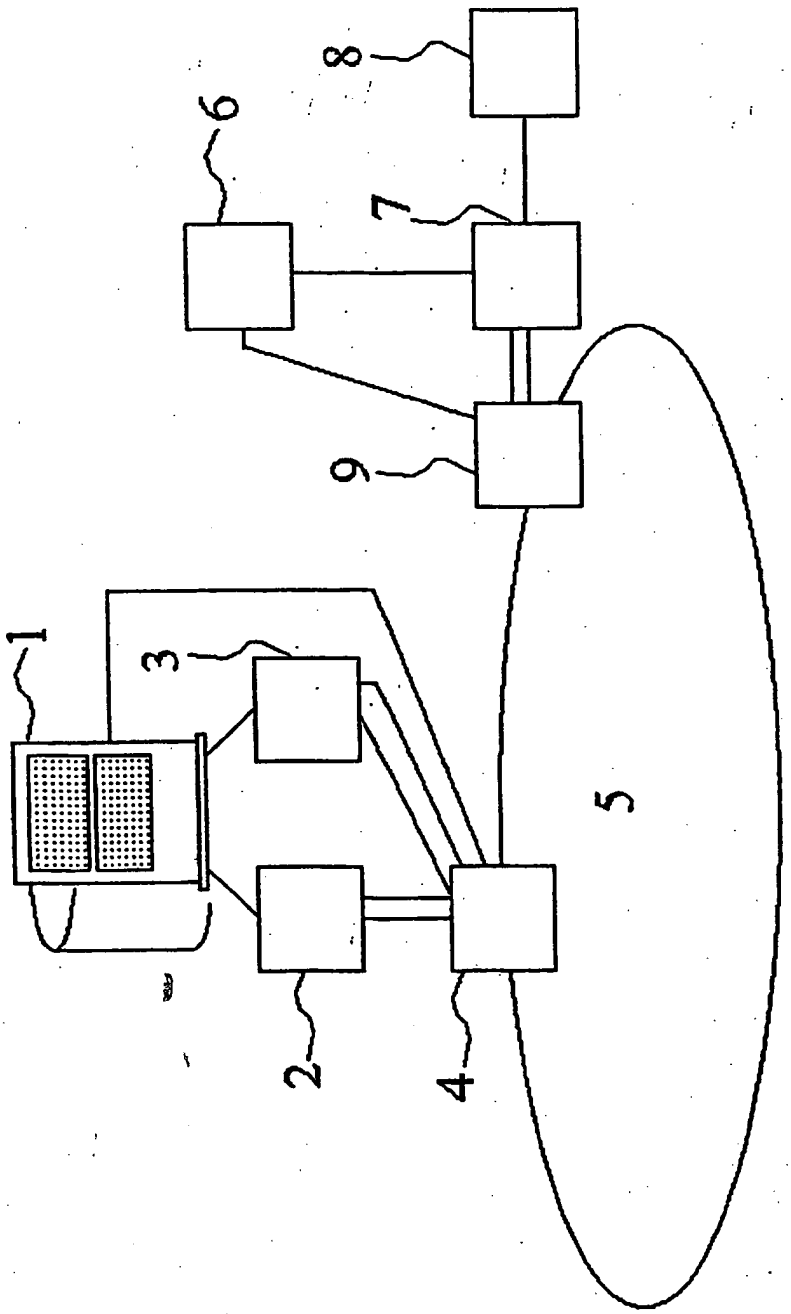
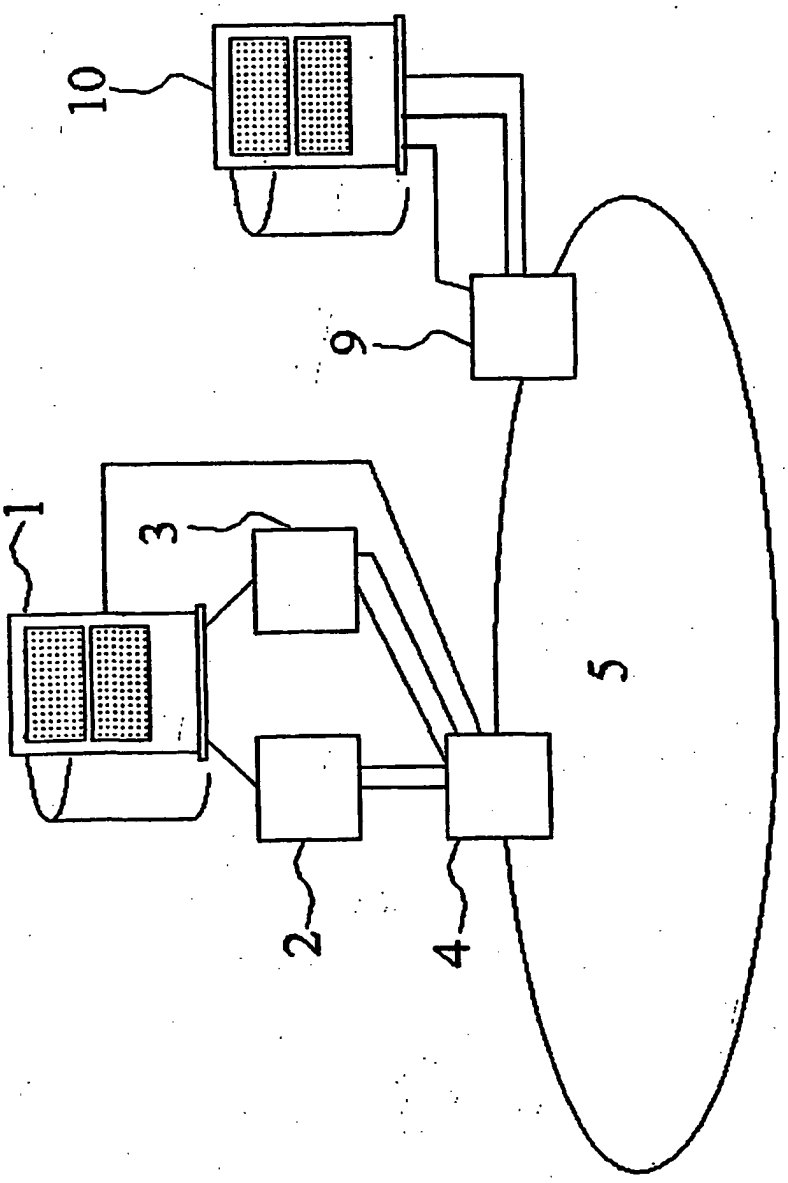


FIG. 2

FIG. 3



INTERNATIONAL SEARCH REPORT

Inter al Application No
PCT/EP 01/06247

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04L12/26

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
- -

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 557 742 A (SMAHA STEPHEN E ET AL) 17 September 1996 (1996-09-17) column 5, line 36 -column 6, line 5; figure 1 column 6, line 61 -column 7, line 3; figure 2B column 11, line 8 - line 23; figure 6B	1-4
A	US 5 796 942 A (ESBENSEN DANIEL) 18 August 1998 (1998-08-18) abstract; figures 1,3 column 3, line 49 -column 4, line 5 column 4, line 60 - line 67 column 5, line 22 - line 34	1-4

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 October 2001	26/10/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Peeters, D

INTERNATIONAL SEARCH REPORT

Inte ial Application No
PCT/EP 01/06247

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 00 05842 A (RAYTHEON CO) 3 February 2000 (2000-02-03) page 2, line 27 - line 30 page 3, line 7 - line 15 page 7; figure 1 page 9, line 17 - line 21 page 6, line 26 - line 28 page 21, line 6 - line 36; figure 6	1-4
A	LUNT T F: "A SURVEY OF INTRUSION DETECTION TECHNIQUES" COMPUTERS & SECURITY. INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY,NL,ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM, vol. 12, no. 4, 1 June 1993 (1993-06-01), pages 405-418, XP000382979 ISSN: 0167-4048 paragraph '0002!	1-4

INTERNATIONAL SEARCH REPORT

ormation on patent family members

Int Application No
PCT/EP 01/06247

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5557742 A	17-09-1996	CA 2144105 A1	08-09-1995
US 5796942 A	18-08-1998	AU 7303198 A	10-06-1998
		CN 1269030 A	04-10-2000
		EP 1008046 A1	14-06-2000
		WO 9822875 A1	28-05-1998
WO 0005842 A	03-02-2000	AU 4953999 A	14-02-2000
		WO 0005842 A1	03-02-2000